The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 34293

September 22, 2022

SEC Sanctions Firm for Violating Regulation S-P by Failing to Properly Dispose of Devices Containing NPPI

[34293]

September 22, 2022

TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Committee
Privacy Issues Working Group
Technology Committee
Transfer Agent Advisory Committee SUBJECTS: Compliance
Fintech and Digital Assets
Litigation & Enforcement
Privacy
Recordkeeping RE: SEC Sanctions Firm for Violating Regulation S-P by Failing to Properly Dispose of Devices Containing NPPI

On September 20, 2022, the SEC settled an enforcement action against a dually-registered broker-dealer and investment adviser for violating Regulation S-P by failing to ensure the proper disposal of customers' non-public personal information (NPPI) when it decommissioned various computer equipment.[1] While the firm neither admitted nor denied the violations, the SEC found that it willfully violated both the Safeguards Rule (Rule 30(a)) and the Disposal Rule (Rule 30(b)) of Regulation S-P through this conduct. As a result, the firm was censured, ordered to cease and desist, and fined $35,000,000. There were no individual respondents named in this action. The facts of this case are briefly summarized below.

The Respondent's Failings

According to the Commission's Order, in 2016, the Respondent retained a Moving Company to decommission its two primary data centers, which were located in New York and Ohio. This decommissioning involved removal of electronic devices (e.g., servers) that contained unencrypted NPPI on customers. While the Moving Company was on the Respondent's list of authorized vendors, it partnered with another corporation to complete this decommissioning. The other corporation was not on the Respondent's list of authorized vendors. While the Respondent's contract with the Moving Company required it to inventory the devices received and their contents and to provide Certificates of Destruction (CODs) evidencing the proper discussion of the devices, the Moving Company failed to do so. Some

of the devices that were decommissioned were sold on the internet. In October 2017, a purchaser of one of these devices, who was an IT consultant in Oklahoma, emailed the Respondent to inform them that he had purchased one of their decommissioned devices from an online auction site "and that he had access to the [firm's] data on those devices." The consultant's email further stated that "you are a major financial institution and should be following some very stringent guidelines on how to deal with retiring hardware. Or at the very least getting some kind of verification of data destruction from the vendors you sell equipment to."

After receipt of this email, the Respondent launched an investigation into the disposition of the devices. Their investigation uncovered back-up tapes from their data centers that had not been accounted for and a lack of documentation that tapes containing data, including NPPI, had, in fact, been destroyed. In July 2020, the Respondent notified approximately 15 million impacted customers that "certain devices believed to have been wiped of all information still contained some unencrypted data," including potential NPPI.

The SEC's Order also found that, between 2015-2017, the Respondent engaged the Moving Company for additional data decommissioning projects for which the Respondent did not comply with its internal policies and procedures and/or maintain documentation sufficient to confirm that its policies were followed. For example, in 2017, the Respondent engaged the Moving Company to decommission 61 servers without going through the required channels for the engagement. Also, the Moving Company provided a COD for the 61 servers but did not specifically identify each of the 244 hard drives that comprised the 61 servers as required by the Respondent's policies and procedures. When the Respondent sought this information, the serial number information provided by the Moving Company did not match the Respondent's records, "raising concerns regarding a possible break in the chain of custody." Because the devices had already been destroyed, the serial numbers could not be readily reconciled. Instead, the Respondent had to reconcile them using information obtained from the servers and hard drive information.

The SEC's Order also discusses the Respondent's use of Wide Area Application Services (WAAS) devices. According to the SEC, these WAAS devices, which were located at the Respondent's local branches, were intended to shorten the amount of time it took branches to access documents by allowing the branches to by-pass the need to access servers located at the data centers. While the WAAS devices were equipped with encryption capability, the Respondent failed to turn on this capability until 2018. Once it was turned on, however, only newly created or overwritten data was encrypted due to a manufacturing flaw in the encryption software. In 2019, the Respondent decommissioned 500 WAAS devices. In February 2020, it realized four devices were missing and discovered the encryption issue. When the Respondent undertook an inventory of its WAAS devices in 2021, it discovered 38 additional devices that could not be located. The Respondent was unable to document the final disposition of its WAAS devices, including CODs and documents evidencing the chain of custody. It also failed to monitor the encryption of data on its WAAS devices. In July 2020 and 2021, the Respondent provided notice to customers potentially impacted by the WAAS breaches.

The SEC's Findings

Based on the above conduct, the SEC found that the Respondent failed to:

- Adopt written policies and procedures that: identified the high level or risk associated with decommissioning devices; required the cataloguing of all decommissioning projects; and governed the resale of decommissioned devices; and

- Reasonably design its policies and procedures governing the employment and monitoring of vendors and sub-vendors to ensure the security and confidentiality of customer records and information.
- Take reasonable measures to protect NPPI of customers or consumer report information when it decommissioned data-bearing devices.

These failures resulted in the Respondent willfully violating Rules 30(a) and (b) of Regulation S-P and imposition of the sanctions discussed above. In settling this case, the Respondent was not required to agree to any undertakings.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See In the Matter of Morgan Stanley Smith Barney, LLC, Administrative Proceeding File No. 3-2112 (September 20, 2022), which is available at: https://www.sec.gov/litigation/admin/2022/34-95832.pdf. The SEC's Press Release on the case is available at: https://www.sec.gov/news/press-release/2022-168.